Frequency Diverse Array Beamforming for Physical-Layer Security with Directionally-Aligned Legitimate User and Eavesdropper

Jingran Lin, Qiang Li, and Jintai Yang
School of Communication and Information Engineering
University of Electronic Science and Technology of China (UESTC), Chengdu China, 611731

***Abstract*—The conventional physical-layer (PHY) security approaches, e.g., transmit beamforming and artificial noise (AN)-based design, may fail when the channels of legitimate user (LU) and eavesdropper (Eve) are close correlated. Due to the highly directional transmission feature of millimeter-wave (mmWave), this may occur in mmWave transmissions as the transmitter, Eve and LU are aligned in the same direction exactly. To handle the PHY security problem with directionally-aligned LU and Eve, we propose a novel frequency diverse array (FDA) beamforming approach to differentiating the LU and Eve. By intentionally introducing some frequency offsets across the antennas, the FDA beamforming generates an angle-range dependent beampattern. As a consequence, it can degrade the Eve's reception and thus achieve PHY security. In this paper, we maximize the secrecy rate by jointly optimizing the frequency offsets and the beamformer. This secrecy rate maximization (SRM) problem is hard to solve due to the tightly coupled variables. Nevertheless, we show that it can be reformulated into a form depending only on the frequency offsets. Building upon this reformulation, we identify some cases where the SRM problem can be optimally solved in closed form. Numerical results demonstrate the efficacy of FDA beamforming in achieving PHY security, even for aligned LU and Eve.**

I. Introduction

As an efficient approach to secure wireless communications, the physical-layer (PHY) security technique has been intensively researched recently [1], [2]. One key performance measure of PHY security is secrecy rate, which is characterized by the channel capacity difference of the legitimate user (LU) and the eavesdropper (Eve). Popular PHY security approaches include transmit beamforming [2]–[4] and artificial-noise (AN)-based designs [5]–[7], which explore certain channel statistical independence to either enhance the LU's reception or jam the Eve's reception.

However, these approaches may fail when the independence assumption does not hold. For instance, there is an increasing attention recently in using millimeter-wave (mmWave) bands for the next generation wireless networks [8]. One important feature of mmWave communications is the highly directional transmission, especially in line-of-sight (LOS) scenarios [9]. Thus, if Eve is aligned with LU in the same transmit direction, highly correlated channels may result. In the worst case, if the Eve's channel vector is a scaled version of the LU's, then the transmit beamforming and AN-aided methods do not work.

To solve the PHY security problem for directionally-aligned LU and Eve, approaches that are able to discriminate LU and Eve with different range in the same transmit direction should be sought. However, to the best of our knowledge, so far no related research has been reported. Frequency diverse array (FDA) is a potential solution to this problem. Basically, FDA employs some small frequency offsets across the antenna array to generate an *angle-range* dependent beampattern [10]. Current research on FDA mainly focuses on analyzing the angle-range dependent beampattern characteristics, and exploring its application in radar and/or navigation systems [11]–[13]. An orthogonal frequency division multiplexing (OFDM) secure transmit scheme is designed in [14], based on FDA with some given and fixed frequency offsets.

Departing from existing research, we propose to employ the FDA technique to achieve PHY security for aligned LU and Eve in highly directional transmissions. To handle such a PHY security problem, we apply FDA's range discrimination capability to enhance the LU's reception and degrade the Eve's. In addition, to maximally explore the array's potential, we further integrate beamforming into FDA and finally develop a novel *FDA beamforming* approach to addressing the directionally-aligned PHY security problem.

Specifically, we maximize the secrecy rate via judiciously designing the FDA beamforming parameters, i.e., the frequency offsets across the array and the transmit beamforming. The secrecy rate maximization (SRM) problem is challenging due to the nonconcave objective and the tightly coupled frequency-offset variables and the beamforming variables. To handle this problem, we first explore the SRM problem structure in order to gain some insights to the FDA beamforming. After that, we develop a two-stage algorithm for this SRM problem, which optimizes the frequency offsets and the transmit beamforming successively. The main difficulty lies in the frequency offsets optimization, which is also a challenging nonconvex problem. Interestingly, we identify some special cases where the problem can be optimally solved. In particular, linearly increasing the frequency across the array attains the maximal secrecy rate. Moreover, the maximal secrecy rate and the optimal frequency offsets can both be computed in closed form.

This work was supported by the National NSFC [61671120, 61401073, and 61471103], and by the Fundamental Research Funds for Central Universities [ZYGX2016J007, ZYGX2016J011].

ISBN 978-0-9928626-7-1

II. System Model and Problem Statement

A. Frequency Diverse Array

As shown in Fig. 1(a), we consider an LOS mmWave communication system consisting of an M-antenna uniform linear transmit array, a single-antenna LU, and a single-antenna Eve. The array forwards confidential information to the LU, in the presence of the Eve overhearing the transmission exactly in the transmit path. To achieve some confidentiality, the FDA beamforming approach is employed to provide PHY security. As opposed to the conventional phase array, FDA introduces small frequency offsets across the array antennas. As shown in Fig. 1(b), the radiation frequency of the mth antenna is $f_m = f_c + \Delta f_m$ for $m = 1, 2, \ldots, M$, with f_c and Δf_m being the carrier frequency and the frequency offsets, respectively. We assume $0 \leq \Delta f_m \leq \Delta F$ and $\Delta F \ll f_c$, where ΔF is the maximal frequency offset. Let d denote the uniform antenna spacing of the transmit array, which is maintained as $d = c/[2(f_c + \Delta F)]$ to avoid aliasing effects with c being the speed of light.

Without loss of generality, we define the first antenna as the origin of the (*range, angle*) coordinate system. Furthermore, to concentrate on the range-dependent SRM problem, we ignore the very few multi-path components (MPCs) in LOS mmWave transmissions, since they were found to be attenuated by 20dB compared to the LOS component [8]. For the user at (r, θ), the LOS channel associated with the mth antenna is given by

$$h_m(f_m, r, \theta) = a(r) e^{-j2\pi(f_c + \Delta f_m)\left[t - \frac{r-(m-1)d\sin\theta}{c}\right]} \quad (1)$$

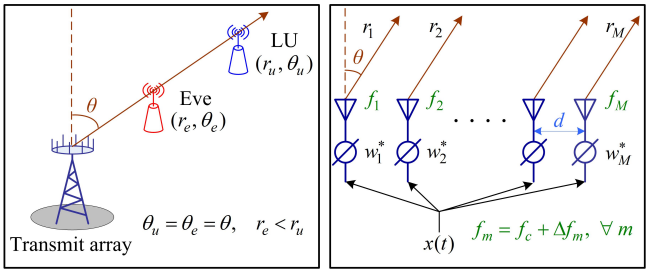
where $a(r)$ denotes the signal attenuation factor at the range of r. Notice that we have assumed far-field model to obtain $h_m(f_m, r, \theta)$, i.e., parallel wavefront and $a(r_m) \simeq a(r)$. For mmWave array transmission, the far-field and LOS assumptions can hold simultaneously due to the tiny array size, usually in magnitude of millimeters.

To focus on the FDA characteristics, we temporarily ignore the attenuation factor $a(r)$ and assume an all-one beamformer. Then, the FDA beampattern at (r, θ) is computed as

$$\begin{aligned} \mathrm{B}(\mathbf{f}, r, \theta) &= \sum\nolimits_{m=1}^{M} h_m(f_m, r, \theta) \\ &= e^{-j2\pi f_c(t - \frac{r}{c})} \sum_{m=1}^{M} e^{-j2\pi\left\{f_c \frac{(m-1)d\sin\theta}{c} + \Delta f_m\left[t - \frac{r-(m-1)d\sin\theta}{c}\right]\right\}} \\ &= e^{-j2\pi f_c(t - \frac{r}{c})} \sum\nolimits_{m=1}^{M} e^{j[\Phi_{0,m}(\theta) + \Phi_{1,m}(\Delta f_m, r, \theta)]} \end{aligned} \quad (2)$$

where $\Phi_{0,m}(\theta) = -2\pi f_c \frac{(m-1)d\sin\theta}{c}$, $\Phi_{1,m}(\Delta f_m, r, \theta) = -2\pi\Delta f_m[t - \frac{r-(m-1)d\sin\theta}{c}]$, $\forall m$, and $\mathbf{f} = [f_1, f_2, ..., f_M]$.

Clearly, the phase terms $\{\Phi_{1,m}(\Delta f_m, r, \theta)\}_{m=1}^{M}$ in (2) depend on the frequency offsets $\{\Delta f_m\}_{m=1}^{M}$, the range r, and the angle θ. By appropriately choosing $\{\Delta f_m\}_{m=1}^{M}$, FDA can generate an *angle-range* dependent beampattern. To show this, we plot the typical beampatterns of the conventional phase array and FDA in Fig. 2. For the sake of simplicity, here we have assumed linearly increasing frequency offsets in FDA, i.e., $\Delta f_m = (m-1)\Delta f$, $\forall m$. In the case of $\Delta f = 0$, we have $\Phi_{1,m}(\Delta f_m, r, \theta) = 0$, $\forall m$, and then FDA reduces to the conventional phase array as shown in Fig. 2(a). As a contrast, we set $\Delta f = 10^{-5} f_c$ in Fig. 2(b) and an *angle-range* dependent beampattern is thus activated owing to the nonzero phase terms $\{\Phi_{1,m}(\Delta f_m, r, \theta)\}_{m=1}^{M}$.



(a) Aligned LU and Eve (b) FDA beamforming

Fig. 1. PHY security based on FDA beamforming for aligned LU and Eve.

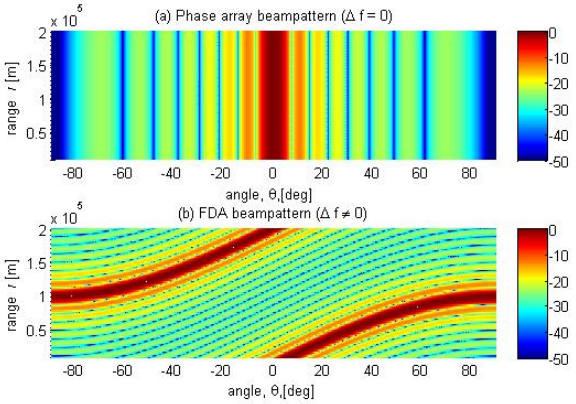


Fig. 2. Typical beampatterns, i.e., $|\mathrm{B}(\mathbf{f}, r, \theta)|$, of phase array and FDA for $M = 8$, $f_c = 60$GHz, and $\Delta f = 600$KHz.

B. Problem Statement

We see from (2) that FDA has a deterministic beampattern for some given $\mathbf{f}$ and time t. In general, there is no guarantee that the LU and Eve are located at the beampattern peak and valley simultaneously. Hence, to maximally explore the array's potentials in PHY security, we further integrate beamforming into FDA, yielding a novel *FDA beamforming* strategy. In particular, let $\mathbf{w} = [w_1, w_2, \ldots, w_M]^T \in \mathbb{C}^{M\times 1}$ denote the array transmit beamformer. The channel vector between the transmit array and the user at (r, θ) is defined as $\mathbf{h}(\mathbf{f}, r, \theta) \triangleq [h_1(f_1, r, \theta), h_2(f_2, r, \theta), \ldots, h_M(f_M, r, \theta)]^T \in \mathbb{C}^{M\times 1}$. The signal-to-noise ratio (SNR) for the user is computed as

$$\mathrm{SNR}(\mathbf{w}, \mathbf{f}, r, \theta) = \sigma^{-2} |\mathbf{w}^\dagger \mathbf{h}(\mathbf{f}, r, \theta)|^2 \quad (3)$$

where σ^2 is the noise power and $(\cdot)^\dagger$ denotes the Hermitian transpose.

Let (r_u, θ_u) and (r_e, θ_e) denote the coordinates of the LU and Eve, respectively. As shown in Fig. 1(a), we have $\theta_u = \theta_e = \theta$ and $r_u > r_e$. To simplify the notations, we use $\mathbf{h}_u(\mathbf{f})$ and $\mathbf{h}_e(\mathbf{f})$ to denote the associated channels, i.e., $\mathbf{h}_u(\mathbf{f}) \triangleq$

ISBN 978-0-9928626-7-1 © EURASIP 2017

$\mathbf{h}(\mathbf{f}, r_u, \theta_u)$ and $\mathbf{h}_e(\mathbf{f}) \triangleq \mathbf{h}(\mathbf{f}, r_e, \theta_e)$. Hence, the achievable LU rate and Eve rate are computed by

$$R_u(\mathbf{w}, \mathbf{f}) = \log(1 + \sigma^{-2}|\mathbf{w}^\dagger \mathbf{h}_u(\mathbf{f})|^2), \quad (4)$$

$$R_e(\mathbf{w}, \mathbf{f}) = \log(1 + \sigma^{-2}|\mathbf{w}^\dagger \mathbf{h}_e(\mathbf{f})|^2). \quad (5)$$

The FDA beamforming based SRM problem is expressed as

$$\max_{\{\mathbf{f},\mathbf{w}\}} \; R_s(\mathbf{w}, \mathbf{f}) \triangleq R_u(\mathbf{w}, \mathbf{f}) - R_e(\mathbf{w}, \mathbf{f}) \quad \text{(P1)}$$

$$\text{s.t.} \;\; \|\mathbf{w}\|_2^2 \le P \quad (6)$$

$$f_c \le f_m \le f_c + \Delta F, \; \forall m \quad (7)$$

with P being the transmit power budget.

III. A Two-Stage Algorithm for SRM Problem

The SRM problem (P1) is challenging due to the nonconcave objective and the tightly coupled variables $\mathbf{f}$ and $\mathbf{w}$. In this section, we first provide some insights to the solution of (P1), and by leveraging these insights we then develop a low-complexity two-stage algorithm to the SRM problem.

A. Some Insights to the Solution of (P1)

To obtain some insights into why FDA can provide PHY security, even for directionally-aligned LU and Eve, let us first fix the frequency variable $\mathbf{f}$ and briefly review the classical PHY secrecy beamforming design [15]. Obviously, with fixed $\mathbf{f}$ in (P1), the SRM problem is the same as the classical multi-input, single-output, single-eavesdropper (MISOSE) secrecy problem in [15], and the optimal beamformer can be computed via generalized eigendecomposition. In particular,

Lemma 1. *[15] Given $\mathbf{f}$ in (P1), let us denote*

$$\mathbf{H}_u(\mathbf{f}) = \tilde{\mathbf{h}}_u(\mathbf{f})\tilde{\mathbf{h}}_u^\dagger(\mathbf{f}), \;\; \tilde{\mathbf{h}}_u(\mathbf{f}) = \sigma^{-1}\mathbf{h}_u(\mathbf{f}) \quad (8)$$

$$\mathbf{H}_e(\mathbf{f}) = \tilde{\mathbf{h}}_e(\mathbf{f})\tilde{\mathbf{h}}_e^\dagger(\mathbf{f}), \;\; \tilde{\mathbf{h}}_e(\mathbf{f}) = \sigma^{-1}\mathbf{h}_e(\mathbf{f}) \quad (9)$$

$$\tilde{\mathbf{H}}_e(\mathbf{f}) = \mathbf{H}_e(\mathbf{f}) + \tfrac{1}{P}\mathbf{I} \quad (10)$$

$$\mathbf{\Sigma}(\mathbf{f}) = \tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f})[\mathbf{H}_u(\mathbf{f}) - \mathbf{H}_e(\mathbf{f})]\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f}). \quad (11)$$

Then, the optimal secrecy rate in (P1) is given by

$$R_s^\star(\mathbf{f}) = \log(1 + [\lambda_{\mathbf{\Sigma}}(\mathbf{f})]^+), \quad (12)$$

where $[\cdot]^+ \triangleq \max\{\cdot, 0\}$ and $\lambda_{\mathbf{\Sigma}}(\mathbf{f})$ is the principle eigenvalue of $\mathbf{\Sigma}(\mathbf{f})$. Moreover, the optimal beamformer $\mathbf{w}^\star$ is given by,

$$\mathbf{w}^\star(\mathbf{f}) = \text{sgn}\{\lambda_{\mathbf{\Sigma}}(\mathbf{f})\} \cdot \sqrt{P}\frac{\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f})\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f})}{\|\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f})\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f})\|_2} \quad (13)$$

where $\text{sgn}\{\cdot\}$ returns 1 if the argument is positive, and 0 otherwise; $\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f})$ is the principle eigenvector of $\mathbf{\Sigma}(\mathbf{f})$.

We should mention that the secrecy rate expression in (12) slightly differs from the original form in [15]. One can easily verify the equivalence between them. We adopt (12) here since it severs our purpose better in the following development.

From (12), we see that the optimal secrecy rate depends on the principle eigenvalue of $\mathbf{\Sigma}(\mathbf{f})$. Since $\mathbf{\Sigma}(\mathbf{f})$ is indefinite in general, $\lambda_{\mathbf{\Sigma}}(\mathbf{f})$ can be either positive or negative. In particular, let us assume $\Delta f_m = 0$ and $\mathbf{f}_p = f_c\mathbf{1}$ with $\mathbf{1}$ being the $M \times 1$ all-one vector; i.e. the conventional phase array beamforming case. For the aligned LU and Eve as shown in Fig. 1(a), we have $\mathbf{h}_e(\mathbf{f}_p) = \alpha\mathbf{h}_u(\mathbf{f}_p)$ with $|\alpha| = \frac{a(r_e)}{a(r_u)} > 1$. Thus, it can be easily concluded that $\mathbf{H}_u(\mathbf{f}_p) - \mathbf{H}_e(\mathbf{f}_p)$ and $\mathbf{\Sigma}(\mathbf{f}_p)$ are negative semidefinite matrices, i.e., $\lambda_{\mathbf{\Sigma}}(\mathbf{f}_p) \le 0$. As a consequence, the conventional beamforming approach fails.

However, by introducing frequency offsets Δf_m across the array antennas, in general we have $\mathbf{h}_e(\mathbf{f}) \neq \alpha\mathbf{h}_u(\mathbf{f})$ due to the nonzero $\{\Phi_{1,m}(\Delta f_m, r, \theta)\}$ in (2). That is, $\mathbf{h}_e(\mathbf{f})$ and $\mathbf{h}_u(\mathbf{f})$ are no longer linearly dependent and $\mathbf{H}_u(\mathbf{f}) - \mathbf{H}_e(\mathbf{f}) \not\succeq \mathbf{0}$. In consequence, $\mathbf{\Sigma}(\mathbf{f})$ may have a positive eigenvalue. Intuitively speaking, the frequency offsets Δf_m play a role of rotating the LU and Eve such that in the rotated space their channels are decorrelated. This key observation not only explains why FDA can provide PHY security even for aligned LU and Eve, it also sheds some lights on how to design the frequency offsets.

According to Lemma 1 and the previous discussion, we see that the SRM problem (P1) boils down to finding the optimal frequency offsets $\Delta f_m, \forall\, m$, such that the principle eigenvalue $\lambda_{\mathbf{\Sigma}}(\mathbf{f})$ is maximized, i.e.,

$$\max_{\mathbf{f}} \;\; \lambda_{\mathbf{\Sigma}}(\mathbf{f}) \quad \text{(P2)}$$

$$\text{s.t.} \;\; f_c \le f_m \le f_c + \Delta F, \; \forall m.$$

After finding the optimal $\mathbf{f}^\star$ for (P2), the optimal beamformer $\mathbf{w}^\star(\mathbf{f}^\star)$ can be computed in closed form based on (13). Thus, in the subsequent development we focus on solving (P2).

Lemma 2. (P2) *is equivalent to the following problem*

$$\min_{\mathbf{f}} \;\; |\langle \mathbf{h}_e(\mathbf{f}), \; \mathbf{h}_u(\mathbf{f})\rangle|^2 \quad \text{(P3)}$$

$$\text{s.t.} \;\; f_c \le f_m \le f_c + \Delta F, \; \forall m$$

where $\langle\cdot,\cdot\rangle$ denotes the inner product.

Proof: Due to space limitation, we only outline the proof here. Basically, we decompose $\tilde{\mathbf{h}}_u(\mathbf{f})$ as

$$\tilde{\mathbf{h}}_u(\mathbf{f}) = \beta\vec{\mathbf{h}}_e(\mathbf{f}) + \gamma\vec{\mathbf{h}}_{e^\perp}(\mathbf{f}) \quad (14)$$

where $\vec{\mathbf{h}}_e(\mathbf{f})$ and $\vec{\mathbf{h}}_{e^\perp}(\mathbf{f})$ are the unit vectors parallel and orthogonal to $\tilde{\mathbf{h}}_e(\mathbf{f})$, respectively; β and γ are scalar numbers satisfying $\beta^2 + \gamma^2 = \|\tilde{\mathbf{h}}_u(\mathbf{f})\|_2^2$. Applying the matrix inverse Lemma, we can express $\lambda_{\mathbf{\Sigma}}(\mathbf{f})$ as a function monotonically decreasing with β^2 for $\beta^2 \in [0, \|\tilde{\mathbf{h}}_u(\mathbf{f})\|_2^2]$. Thus, maximizing $\lambda_{\mathbf{\Sigma}}(\mathbf{f})$ is equivalent to minimizing β^2. Since $|\langle \mathbf{h}_e(\mathbf{f}), \mathbf{h}_u(\mathbf{f})\rangle|^2 = \beta^2\|\mathbf{h}_e(\mathbf{f})\|_2^2 = Ma^2(r_e) \cdot \beta^2$, we establish the equivalence between (P2) and (P3). ■

Lemma 2 reveals that the optimal frequency offsets should turn the channels of LU and Eve as orthogonal as possible. In the ideal case, we should have $\langle \mathbf{h}_e(\mathbf{f}), \; \mathbf{h}_u(\mathbf{f})\rangle = 0$. However, due to the limited dynamic range of the frequency offsets, it is in general not possible to make $\mathbf{h}_e(\mathbf{f})$ and $\mathbf{h}_u(\mathbf{f})$ orthogonal exactly. Next, we will identify some special cases, under which the orthogonality can be guaranteed.

B. Closed-form Solution for (P3) under Some Special Cases

Intuitively, if there is sufficient flexibility to choose f_m, i.e., ΔF is large enough, we would expect that $\mathbf{h}_e(\mathbf{f})$ and $\mathbf{h}_u(\mathbf{f})$ can be turned orthogonal exactly. The following propositions formalize this idea.

ISBN 978-0-9928626-7-1 © EURASIP 2017

Proposition 1. *Suppose $\theta_u = \theta_e$ and $\Delta F \geq \frac{(M-1)c}{M(r_u - r_e)}$. Then,* (P3) *can be optimally solved. Specifically, the optimal solution, denoted by $\mathbf{f}^\star = [f_1^\star, f_2^\star, \ldots, f_M^\star]$, is given by*

$$f_m^\star = f_c + (m-1)\Delta f^\star, \text{ and } \Delta f^\star = \frac{c}{M(r_u - r_e)}, \ \forall\ m. \quad (15)$$

Moreover, at the optimal solution, $\mathbf{h}_u(\mathbf{f}^\star)$ and $\mathbf{h}_e(\mathbf{f}^\star)$ are orthogonal, i.e., $\langle \mathbf{h}_e(\mathbf{f}^\star), \mathbf{h}_u(\mathbf{f}^\star)\rangle = 0$, and the optimal secrecy rate is $R_s^\star(\mathbf{f}^\star) = \log[1 + \frac{a^2(r_u)PM}{\sigma^2}]$.

Proof: According to the definition of the directional channels $\mathbf{h}_u(\mathbf{f})$ and $\mathbf{h}_e(\mathbf{f})$, we have

$$\begin{aligned}\langle \mathbf{h}_e(\mathbf{f}), \mathbf{h}_u(\mathbf{f})\rangle &= a(r_e)a(r_u)\sum_{m=1}^{M} h_m^*(f_m, r_e, \theta)h_m(f_m, r_u, \theta) \\ &= a(r_e)a(r_u)e^{j2\pi f_c \frac{(r_u - r_e)}{c}} \sum\nolimits_{m=1}^{M} e^{j2\pi \Delta f_m \frac{(r_u - r_e)}{c}} \quad (16)\end{aligned}$$

For linearly increasing frequency offsets, i.e., $\Delta f_m = (m-1)\Delta f$, $m = 1, 2, ..., M$, we have

$$\begin{aligned}\sum\nolimits_{m=1}^{M} e^{j2\pi \Delta f_m \frac{r_u - r_e}{c}} &= \sum\nolimits_{m=1}^{M} e^{j2\pi (m-1)\Delta f \frac{(r_u - r_e)}{c}} \\ &= \frac{\sin\left[\frac{M\pi \Delta f (r_u - r_e)}{c}\right]}{\sin\left[\frac{\pi \Delta f (r_u - r_e)}{c}\right]} e^{j\pi (M-1)\Delta f \frac{(r_u - r_e)}{c}} \quad (17)\end{aligned}$$

Therefore, when

$$\Delta f^\star = \frac{kc}{M(r_u - r_e)}, \quad k = \pm 1, \ \pm 2, \ ... \quad (18)$$

we have $\langle \mathbf{h}_e(\mathbf{f}^\star), \mathbf{h}_u(\mathbf{f}^\star)\rangle = 0$ and thus the optimality of (P3) is achieved. In practice, we use the smallest positive frequency offset $\Delta f^\star = \frac{c}{M(r_u - r_e)}$.

The fact $\langle \mathbf{h}_e(\mathbf{f}^\star), \mathbf{h}_u(\mathbf{f}^\star)\rangle = 0$ indicates the orthogonality between $\mathbf{h}_u(\mathbf{f}^\star)$ and $\mathbf{h}_e(\mathbf{f}^\star)$. Using this result, one can easily verify that the maximum eigenvalue of $\mathbf{\Sigma}(\mathbf{f})$ is $P\|\tilde{\mathbf{h}}_u(\mathbf{f}^\star)\|_2^2$ or $\frac{a^2(r_u)PM}{\sigma^2}$. Equivalently, the corresponding optimal secrecy rate is $R_s^\star(\mathbf{f}^\star) = \log[1 + \frac{a^2(r_u)PM}{\sigma^2}]$. ■

Remark 1. *Under the conditions of Proposition 1, the maximum secrecy rate is $\log[1 + \frac{a^2(r_u)PM}{\sigma^2}]$, which is the maximum channel capacity of LU (without Eve). Therefore, the presence of Eve does not degrade the rate performance between transmitter and LU.*

Remark 2. *Given the maximum frequency offset range ΔF, the conditions in Proposition 1 impose a minimum distance between LU and Eve, i.e., $|r_u - r_e| \geq \frac{(M-1)c}{M\Delta F}$, to achieve the optimality.*

Proposition 1 reveals an interesting result. For directionally aligned LU and Eve (with sufficiently large ΔF), linearly increasing frequency offsets across the array is optimal. Actually, the optimality of linear frequency offset can be generalized to the case of $\theta_u \neq \theta_e$ under some mild conditions.

Proposition 2. *Suppose $\Delta f_m \ll f_c$, $\forall\ m$, $d \ll |r_u - r_e|$, and $\Delta F \geq (M-1)\Delta \tilde{f}$, where $\Delta \tilde{f} = \frac{kc + Mf_c d(\sin\theta_u - \sin\theta_e)}{M(r_u - r_e)}$ and k is the smallest nonzero integer satisfying $\Delta \tilde{f} > 0$. Then, linearly increasing frequency offset is optimal and the optimal frequency offset is given by*

$$f_m^\star = f_c + (m-1)\Delta f^\star \text{ and } \Delta f^\star = \Delta \tilde{f}, \ \forall\ m. \quad (19)$$

Proof: We omit the details of proof due to space limitation. Basically, Proposition 2 can be proved similarly as Proposition 1 except that we ignore the phase term $\frac{\Delta f_m (m-1) d(\sin\theta_u - \sin\theta_e)}{c}$ in $\langle \mathbf{h}_e(\mathbf{f}),\ \mathbf{h}_u(\mathbf{f})\rangle$ due to the conditions of $d \ll (r_u - r_e)$ and $\Delta f_m \ll f_c$. ■

We remark the conditions of $d \ll |r_u - r_e|$ and $\Delta f_m \ll f_c$ are mild and usually hold in practice in order to avoid aliasing and decorrelation effects in FDA transmission.

We also remark that (15) is actually a special case of (19) as $\theta_e = \theta_u$. Therefore, the FDA beamforming strategy possesses discrimination capabilities in both direction and range.

C. Two-Stage Algorithm

We summarize the two-stage algorithm for the FDA beamforming based SRM problem in Table 1. In the first stage, we optimize the frequency offsets across the antennas to rotate the channels of LU and Eve as orthogonal as possible. Specifically, for the identified special cases, the optimal frequency offsets can be obtained; for the general case, however, we develop an iterative algorithm utilizing the block successive upper-bound minimization (BSUM) method to find a solution for frequency offsets with stationary convergence guarantee [16]. This is not covered in this paper due to space limitation. The details can be found in the journal version [16] (submitted to IEEE TIFS). In the second stage, the beamformer is optimized based on the given frequency offsets according to (13).

Table 1: Two-stage Algorithm for SRM Problem

(1)	Initialize the system parameters	
(2)	[Stage 1]	Optimize the frequency increments
(3)		Calculate $\Delta \tilde{f} = \frac{kc + Mf_c d(\sin\theta_u - \sin\theta_e)}{M(r_u - r_e)}$
		k is the smallest integer such that $\Delta \tilde{f} > 0$;
(4)		***if*** $\Delta F \geq (M-1)\Delta \tilde{f}$,
		output $f_m^\star = f_c + (m-1)\Delta \tilde{f}$, $\forall m$;
(5)		***else***, find a stationary solution $f_m^\star$, $\forall m$ [16];
(6)	[Stage 2]	Optimize the beamformer
(7)		$\mathbf{w}^\star = \text{sgn}\{\lambda_{\mathbf{\Sigma}}(\mathbf{f}^\star)\} \cdot \frac{\sqrt{P}\tilde{\mathbf{H}}_e^{-1/2}(\mathbf{f}^\star)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f}^\star)}{\|\tilde{\mathbf{H}}_e^{-1/2}(\mathbf{f}^\star)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f}^\star)\|_2}$,
(8)	Output the secrecy rate $R_s^\star(\mathbf{f}^\star) = \log[1 + \lambda_{\mathbf{\Sigma}}(\mathbf{f}^\star)]$.	

We should mention that the two-stage algorithm is done in one shot and there is no alternating between the frequency and beamformer optimization. With each step being solved analytically, the two-stage algorithm can be performed efficiently.

IV. Simulation and Conclusion

We consider an LOS mmWave communication system operating at $f_c = 60$GHz. The system consists of an M-antenna transmit array, a single-antenna LU and a single-antenna Eve. We assume -100dBm receive noise power for LU and Eve, i.e., $10\log(\sigma^2) = -100$dBm. The signal attenuation factor $a(r)$ is determined by the free-space path loss formula of radio wave propagation, i.e.,

$$\begin{aligned}\text{Lfs (dB)} &= -20\log[a(r)] \\ &= 32.5 + 20\log[F(\text{MHz})] + 20\log[r(\text{Km})] \quad (20)\end{aligned}$$

where $F \simeq f_c$ is transmit frequency in megahertz (MHz), and r is the range in kilometer (Km). We fix the LU's coordinate

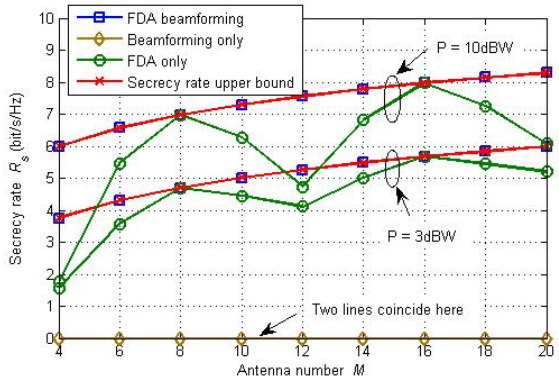


Fig. 3. Secrecy rate comparison for different antenna numbers M at $r_u = 1000m$, $r_e = 500m$, and $\theta_u = \theta_e = 30^{\rm o}$.

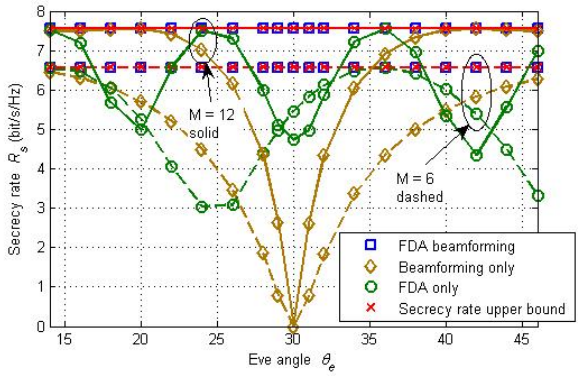


Fig. 4. Secrecy rate comparison for different Eve angles θ_e at $r_u = 1000m$, $\theta_u = 30^{\rm o}$, $r_e = 500m$, and $P = 10$dBW.

as $(r_u, \theta_u) = (1000m, 30^{\rm o})$, and change the other parameters to test the algorithm's performance in different aspects.

First, we set $(r_e, \theta_e) = (500m, 30^{\rm o})$, $\Delta F = \frac{c}{|r_u - r_e|}$, and compare the performances of the following 3 algorithms: (1) the proposed FDA beamforming algorithm (cf. Table 1); (2) the pure beamforming algorithm, which employs the optimal beamformer of (13) with fixed $\mathbf{f} = f_c\mathbf{1}$, i.e., $\Delta f_m = 0$, $\forall\ m$; (3) the pure FDA algorithm without beamforming, where the array transmits with the fixed beamformer $\mathbf{w} = \sqrt{P/M}\cdot\mathbf{1}$, and the stepped frequency offset Δf is determined by performing one-dimension search in the range of $[0, \Delta F]$.

The secrecy rate comparison for different antenna numbers M is illustrated in Fig. 3, where we also plot the theoretical secrecy rate upper bound $\log[1 + \frac{a^2(r_u)PM}{\sigma^2}]$. When the LU and Eve are directionally aligned, the pure beamforming fails. Performing frequency offsetting yields some positive secrecy rate. However, there is no guarantee that the improved secrecy rate can be achieved without optimizing the beamformer. The proposed FDA beamforming algorithm always achieves the secrecy rate upper bound by jointly optimizing the frequency offsets and the transmit beamformer.

Next, we fix the Eve's range as $r_e = 500m$ and change its angle θ_e. The secrecy rate comparison is illustrated in Fig. 4, where we used the stepped frequency offset $\Delta\tilde{f}$ in Proposition 2 in the FDA beamforming algorithm. As θ_e departs from θ_u, the channels associated with LU and Eve may span different subspaces. Therefore, the pure beamforming algorithm begins to work gradually. The pure FDA algorithm behaves unstably, depending on the FDA beampattern shape. The proposed FDA beamforming algorithm exhibits a stable performance, which achieves the secrecy rate bound regardless of θ_e.

In summary, an innovative FDA beamforming approach is proposed for the directionally-aligned PHY security problem. Specifically, we aim to maximize the secrecy rate by optimizing the frequency offsets and the transmit beamformer jointly. After providing some insights to the FDA beamforming, we design a two-stage algorithm to solve the challenging problem. In our solution development, we further identify some special cases, under which the SRM problem can be optimally solved in closed form.

REFERENCES

[1] Y. Liang, H.V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communication and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2008.

[2] A Mukherjee, S. Fakoorian, J. Huang, and A.L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.

[3] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel state information," *IEEE Trans. Vehicular Technology*, vol. 62, no. 3, pp. 2140–2155, June 2013.

[4] S. Gerbracht, C. Scheunert, and E.A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[5] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-atenna multi-relay networks," *IEEE Trans. Signal Processing*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

[6] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[7] X. Zhang, X. Zhou and M.R. Mckay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Vehicular Technology*, vol. 62, no. 5, pp. 2170–2181, May 2013.

[8] MiWEBA, "Millimetre-wave evolution for backhaul and access," *MiWEBA Technical Reports*, June 2014.

[9] S. Rangan, T.S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," in *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

[10] P. Antonik, M.C. Wicks, H.D. Griffiths, and C.J. Baker, "Frequency diverse array radars," in *Proc. IEEE Radar Conf.*, pp. 215-217, Verona, April 2006.

[11] W.-Q. Wang, "Overview of frequency diverse array in radar and navigation applications," *IET Radar, Sonar & Navigation*, vol. 10, no. 6, pp. 1001–1012, Jun. 2016.

[12] S. Mustafa, D. Simsek, and H.A.E. Taylan, "Frequency diverse array antenna with periodic time modulated pattern in range and angle," in *Proc. IEEE Radar Conf.*, pp. 427–430, Boston, April 2007.

[13] P.F. Sammartino, C.J. Baker, and H.D. Griffiths, "Frequency diverse MIMO techniques for radar," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 201–222, Jan. 2013.

[14] Y. Ding, J. Zhang and V. Fusco, "Frequency diverse array OFDM transmitter for secure wireless communication," *Electronic Letters*, vol. 51, no. 17, pp. 1374–1376, Aug. 2015.

[15] A. Khisti and G.W. Wornell, "Secure transmission with multiple antennas I: the MISOME wiretap channel," *IEEE Trans. Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[16] J. Lin, Q. Li, J. Yang, H. Shao and W.-Q. Wang, "Physical-layer security for directionally-aligned legitimate user and eavesdropper: a frequency diverse array beamforming approach," submitted to *IEEE Trans. Information Forensics and Security*.

ISBN 978-0-9928626-7-1 © EURASIP 2017